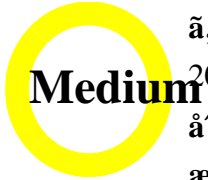


# Cisco IOS XR PIM, SPT, and Protocol Independent Multicast

## Medium Severity Vulnerability in Cisco IOS XR PIM



Cisco Security Advisory ID : cisco-sa-20190417-iosxr-pim-dos

[CVE-2019-1712](#)

Published : 2019-04-17 16:00

Revised : 2019-06-28 13:51

Version : 1.2 : Final

CVSS Score : [5.8](#)

Impact : Yes

Cisco ID : [CSCvg43676](#)

**Medium Severity Vulnerability in Cisco IOS XR PIM**

**Medium**

Cisco IOS XR PIM, SPT, and Protocol Independent Multicast

IP PIM SPT and Protocol Independent Multicast (PIM) AutoRP

Severity: Medium

The vulnerability exists in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components of Cisco IOS XR. It is a Denial of Service (DoS) vulnerability. The vulnerability is caused by a buffer overflow in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components. An attacker can exploit this vulnerability by sending a specially crafted packet to the affected device, which will cause a buffer overflow and a denial of service.

The vulnerability is caused by a buffer overflow in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components. An attacker can exploit this vulnerability by sending a specially crafted packet to the affected device, which will cause a buffer overflow and a denial of service.

The vulnerability is caused by a buffer overflow in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components. An attacker can exploit this vulnerability by sending a specially crafted packet to the affected device, which will cause a buffer overflow and a denial of service.

The vulnerability is caused by a buffer overflow in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components. An attacker can exploit this vulnerability by sending a specially crafted packet to the affected device, which will cause a buffer overflow and a denial of service.

The vulnerability is caused by a buffer overflow in the PIM SPT and Protocol Independent Multicast (PIM) AutoRP components. An attacker can exploit this vulnerability by sending a specially crafted packet to the affected device, which will cause a buffer overflow and a denial of service. <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-iosxr-pim-dos>

CVSS Score: 5.8

Impact: Yes

Published: 2019-04-17 16:00





æœ-ã,çãf%ãfã,ã,ã,ãfãã®è~èç°ãt...ã®¹ã«é-çã—ã|æf...ã±é...ãzjã® URL  
ã,çœç•¥ã—ã€ããç<-ã®è»çè¼%ã,,æ,,è³ã,'æ-½ã—ãÿã'ã^ã€ã½"ç³¼ãÇç®;ç  
ã"ã®ãf%ã,ãf¥ãf;ãf³ãf^ã®æf...ã±ã-ã€ã,ã,ã,ã,³è£½ã"ã®ã,ãf³ãf%ãf!ãf¼ã,ã,ã,ã³¼è±;ã

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。